FEATURE: INSIDER THREAT IS NOW CONVICTED

Trusted and Betrayed: Cybersecurity Professionals Sentenced for BlackCat Ransomware Attacks

May 1, 2026 | uMercs Intelligence Team

The U.S. Department of Justice sentenced two cybersecurity professionals to four years in federal prison for facilitating BlackCat (ALPHV) ransomware attacks throughout 2023. Ryan Goldberg, an incident response manager at Sygnia, and Kevin Martin, a consultant at DigitalMint, pleaded guilty in December 2025 -- conspiring with Angelo Martino, a ransomware negotiator who secretly aided the attackers while ostensibly helping their victims.

The trio paid BlackCat RaaS operators a 20% cut of all ransoms. In one case, they successfully extorted a victim for approximately $1.2 million in Bitcoin, splitting their 80% share and laundering the proceeds to cover their tracks. Martino, still awaiting sentencing in July 2026, is accused of sharing victims' insurance policy limits with the attackers to inflate payout demands -- a move that turned a negotiation into a shakedown.

This case redraws the insider threat map. It confirms that the risk isn't limited to disgruntled employees or compromised admins -- it extends to the trusted third parties organizations bring in to handle their worst day. An IR manager and a ransomware negotiator both had badges, credentials, and years of legitimate security work behind them. They also had ransomware payloads.

The structural vulnerability here is access scoping. During an active incident, IR vendors receive broad, often unmonitored privileges -- credentials, system access, network visibility, and critically, knowledge of insurance limits and negotiation posture. Very few organizations audit that access in real time, and fewer still revoke it systematically post-engagement.

What defenders should do:

- Vet third-party IR vendors as rigorously as privileged internal employees
- Compartmentalize insurance policy data -- restrict access to named individuals only
- Implement just-in-time access provisioning for IR engagements
- Monitor IR vendor activity in real time during engagements -- not just pre-engagement vetting
- Conduct formal access revocation reviews within 48 hours of incident closure
- Treat negotiators as potential insider threats until proven otherwise

RANSOMWARE BRIEF

Clop Still Hunting Oracle Customers

Clop ransomware continues active exploitation of CVE-2025-61882 in Oracle environments. Unpatched Oracle systems remain prime targets heading into Q2 2026. If your Oracle infrastructure hasn't been assessed since Q4 2025, consider it at risk.

BlackCat Legacy Lingers

Despite its official law enforcement takedown, BlackCat infrastructure and ransomware code remain active through former affiliates and forks. The Goldberg/Martin case confirms that the gang's reach extended deep into legitimate security firms -- the cleanup is not complete.

Akira Exploiting SonicWall SMA100

Akira ransomware is actively exploiting SonicWall SMA100 vulnerabilities (CVE-2025-40596 through CVE-2025-40599), including on devices reporting as fully patched. Independently verify your SMA100 firmware -- don't trust the dashboard.

VMware ESXi Under Ransomware Fire

CVE-2025-22225 (VMware ESXi arbitrary write) continues to be leveraged in ransomware campaigns despite Broadcom patching it in March 2025. Hypervisor compromise = entire estate at risk. Validate ESXi patch status across all hosts.

BY THE NUMBERS

1,000+
BlackCat victims globally before shutdown

$1.2M
Single payout extorted by the convicted IR team

CVE-2026-32202

ConnectWise ScreenConnect RCE | CVSS 9.8 Critical

Path traversal allows unauthenticated remote code execution. Added to CISA KEV April 28 with a federal patching deadline of May 12. Affects all versions before 25.3.1. A compromised ScreenConnect server is a direct pivot point into every endpoint it manages -- MSPs and IT teams should treat this as emergency priority.

CVE-2026-32202 (Windows Shell)

Windows Shell -- APT28 Patch Bypass | CVSS High

Microsoft initially patched this flaw, then confirmed active exploitation by APT28 (Russian GRU) via a bypass of that patch. A second, revised patch has been issued. Federal deadline May 12 via CISA KEV. Non-federal orgs: apply immediately given confirmed nation-state exploitation in the wild.

April 2026 Patch Tuesday

165 CVEs -- Second Largest PT Ever | CVSS Multiple Critical

April 2026 PT addressed 165 CVEs -- Microsoft's second-largest update in history. Highlights: CVE-2026-33824 critical IKE RCE (double-free, no-auth), three zero-days, Entra ID service principal takeover, and post-release exploitation confirmation of Windows Shell. Prioritize IKE and Entra ID patches immediately.

uMercs Threat Intel
May 2026 | Vol. 3 | Monthly Intelligence Digest
OFFENSIVE SECURITY INTEL
umercs.com

GEO INTEL: NATION-STATE ACTIVITY

Operation Epic Fury Aftermath & the Iranian Cyber Posture Shift

Analysis | uMercs Intelligence Team

The aftermath of U.S. Cyber Command's Operation Epic Fury continues to reshape the threat landscape. The pre-kinetic cyber strikes that preceded the first U.S. airstrikes on Iranian nuclear facilities disrupted command-and-control infrastructure and GPS spoofing operations, forcing Iran to pivot maritime navigation systems from GPS to China's BeiDou network. Over 1,100 ships have since reported GPS spoofing events affecting commercial navigation.

As Iranian proxy groups scramble to rebuild C2 infrastructure, security researchers are tracking a surge in phishing campaigns, credential theft operations, and watering hole attacks attributed to IRGC-aligned actors. Primary targets include U.S. defense contractors, government-adjacent firms, and organizations in the energy and critical infrastructure sectors.

Chinese threat actor UAT-8837 remains persistently active, exploiting a Sitecore CMS vulnerability to target North American critical infrastructure. The group has demonstrated patience and precision -- dwell times measured in months, not days. Separately, Silk Typhoon's extradition to the U.S. in connection with COVID research cyberattacks marks a rare enforcement win, but the group's TTPs are widely replicated across affiliated clusters.

The broader pattern: geopolitical events are directly accelerating offensive cyber operations. The window between a real-world escalation and an associated cyber campaign is now measured in hours. Organizations in defense, energy, healthcare, and government contracting supply chains should treat the current period as elevated threat posture.

Active Threat Actor Watch:

- **APT28 (Russia/GRU):** Active exploitation of patched Windows Shell flaw via bypass
- **UAT-8837 (China):** Sitecore exploitation, critical infrastructure, long dwell
- **IRGC Proxies (Iran):** Credential theft surge and C2 rebuild post-Epic Fury
- **Silk Typhoon (China):** Indicted; TTPs remain circulating in affiliated groups
- **Clop:** Oracle exploitation ongoing; financially motivated, high-volume

PATCH TUESDAY DEEP DIVE

April 2026 -- What Matters Most

CVE-2026-33824 -- IKE RCE

Critical double-free vulnerability in Windows Internet Key Exchange (IKE) extension. Allows remote code execution with no authentication required. Any internet-facing Windows system using IKE/IPsec is exposed. Patch immediately.

CVE-2026-32202 -- Windows Shell

APT28 confirmed active exploitation AFTER Microsoft's initial patch via a bypass. A second revised patch is required. Treat this as an unpatched zero-day until your security team independently verifies the second patch is applied.

Microsoft Entra ID Role Flaw

Service Principal takeover vulnerability -- patched in April PT. Audit all Entra ID service principal permissions post-patch. Overprivileged SPs are a persistent Azure attack surface that organizations consistently underestimate.

cPanel Auth Bypass -- Critical

Critical authentication bypass across multiple cPanel authentication paths. Trivially exploitable. MSPs and hosting providers using cPanel should patch immediately and audit for signs of unauthorized access since April 15.

SUPPLY CHAIN ALERT

Checkmarx / Bitwarden CLI Compromise

Malicious Docker images and VS Code extensions were confirmed in a Checkmarx supply chain attack. The Bitwarden CLI was also compromised in the same campaign. If Bitwarden CLI is in any of your CI/CD pipelines or developer toolchains, rotate all related credentials and audit pipeline logs from March 23 onward.

GitHub CVE-2026-3854 -- RCE via Git Push

Researchers discovered a critical RCE vulnerability in GitHub exploitable via a single malicious git push. If you run self-hosted GitHub Enterprise, patch immediately. Cloud-hosted GitHub was patched server-side -- no action required for github.com users.

MAY 2026 DEFENDER CHECKLIST

[ ] Patch ConnectWise ScreenConnect to v25.3.1 -- CISA KEV deadline May 12
[ ] Apply Microsoft's SECOND Windows Shell patch -- APT28 bypassed the first one
[ ] Patch IKE RCE (CVE-2026-33824) -- no-auth RCE, treat as critical
[ ] Update cPanel immediately -- auth bypass is trivially exploitable, check access logs
[ ] Audit CI/CD pipeline: remove or pin Bitwarden CLI and Checkmarx dependencies
[ ] Rotate credentials if Bitwarden CLI was in your toolchain (exposure window: March 23+)
[ ] Review IR vendor / negotiator access -- insider threat controls are not optional
[ ] Audit Entra ID service principal permissions post-April Patch Tuesday
[ ] Independently verify SonicWall SMA100 firmware -- Akira exploiting even 'patched' devices
[ ] Validate VMware ESXi patch status across all hypervisor hosts (CVE-2025-22225)

uMercs Threat Intel
May 2026 | Vol. 3 | Monthly Intelligence Digest
OFFENSIVE SECURITY INTEL
umercs.com

CYBER TIP: VETTING YOUR INCIDENT RESPONDERS

Trust, But Verify -- Even the People You Hired to Verify

The BlackCat sentencing isn't just a law enforcement story. It's a procurement story. Goldberg and Martin worked for recognized security firms. They had badges, industry certifications, and years of legitimate incident response experience. They also had ransomware binaries. The lesson isn't to distrust all IR vendors -- it's to build structural controls that don't depend on vendor trustworthiness alone.

When an incident occurs, organizations are under pressure. The IR vendor gets called, given broad system access, and handed the keys -- sometimes literally. That access is rarely scoped tightly, rarely monitored in real time, and almost never audited post-engagement. That's the gap the Goldberg/Martin case exploited.

The fix is process, not paranoia. Just-in-time access provisioning means IR vendors get credentials when they need them and they expire when they don't. Read-only investigation environments for initial triage prevents lateral movement under the guise of forensics. Tiered credentialing separates diagnostic access from remediation access. And post-engagement access revocation reviews -- within 48 hours of closure -- ensure nothing lingers.

One more thing: compartmentalize your insurance policy. The number one intelligence asset Martino weaponized wasn't a zero-day -- it was knowing the victim's coverage limit. That information should be held by a named individual or two, not broadly shared during an active incident response engagement.

THREAT CONTEXT: AI IS COLLAPSING THE EXPLOIT WINDOW

13 Hours From Disclosure to Exploitation

LMDeploy CVE-2026-33626 was discovered and exploited in the wild within 13 hours of public disclosure. Anthropic's Claude Mythos launched April 7 and immediately changed the velocity of vulnerability research -- AI-assisted discovery is outpacing human-only research by an order of magnitude, but creating a remediation backlog that security teams weren't designed to absorb at that speed.

The FIRESTARTER backdoor survived patching on a federal Cisco Firepower device -- a reminder that sophisticated attackers don't wait for you to notice. The gap between 'patch released' and 'environment secured' is where breaches happen. That gap is now measured in hours.

This is why uMercs built AI pentest agents. Continuous, autonomous testing against your real environment doesn't wait for the annual assessment window. It runs every day. The agents are live now -- covering network infrastructure, web applications, Active Directory, and credential attack chains -- and getting better every week.

SOURCES

- The Hacker News (thehackernews.com)
- CISA KEV Catalog (cisa.gov/kev)
- SANS ISC Diary Archive (isc.sans.edu)
- BleepingComputer (bleepingcomputer.com)
- Arctic Wolf / Qualys / Talos / SC Media
- CyberScoop / SecurityWeek / Dark Reading
- DOJ Press Release (May 1, 2026)
- abhs.in CVE-2026-32202 analysis

THIS MONTH IN INFOSEC

"So the incident responder was also the ransomware operator?"
"Correct. He was negotiating against himself."

"Did the ransom go up?"
"He had excellent intelligence on the victim's insurance limits. So yes. Significantly."

"Where does it end?"
"Four years in federal prison, apparently. Though the irony remains unpatched."

-- No technical humor was harmed in the writing of this panel. One $1.2M payout was.